

COMMITTEE ON GOVERNMENT REFORM



MEDIA ADVISORY

For Immediate Release
October 14, 2003

Contact: David Marin
(202) 225-5074

You've got mail -- but is it secure? ***Government Reform Committee to Examine Internet Vulnerabilities Affecting Businesses, Governments, and Homes***

How can governments, businesses and home users
better prepare for and respond to worms and viruses?

What can we do to better educate the public about the growing cyber threat?

Do e-government initiatives make us all more vulnerable to cyber attacks?

Is our critical infrastructure particularly vulnerable to a potential terrorist attack?

WHAT: GOVERNMENT REFORM COMMITTEE OVERSIGHT HEARING:
"You've Got Mail -- But Is It Secure? An Examination of Internet Vulnerabilities
Affecting Businesses, Governments, and Homes."

WHEN: Thursday, October 16, 2003, 10:00 a.m.

WHERE: 2154 RAYBURN HOUSE OFFICE BUILDING

"Unfortunately, the power of the Internet can be exploited for evil as well as good, a phenomenon that is not atypical for such a great advance in technology. And the Internet is particularly vulnerable to the exploits of those with malevolent intentions."

- Dr. F. Thomson Leighton, Chief Scientist, Akamai Technologies Inc.
Professor of Applied Mathematics, MIT

Background:

At this hearing, the Committee will examine the Internet's vulnerabilities and the threat they pose to our national security, public health and safety, and economy.

Akamai Technologies, Inc. will give a demonstration of the “Slammer” worm’s effect in elapsed time and its estimated impact on individual computers and networks. A presentation from NetSec will show the ease with which the average computer user can obtain names, Social Security numbers and other sensitive information through popular search engines like Google.

Citizens, businesses, and governments rely on the Internet for a variety of activities: business transactions, acquisition of goods and services, and the collection and dissemination of information to name a few. Therefore, the Committee will review what steps these groups are taking to create a more secure cyber-environment, with particular attention to the Federal government’s response to this growing cyber-threat.

As we have seen in recent months, computer viruses and worms can cause significant damage to home and work computers. Loss of files and data may cause irreparable financial damage, mar a business’ reputation, and even shut down operations in a private or government enterprise. Furthermore, hackers are able to divert traffic from websites and steal information, including personally identifiable information, patients’ medical records, and financial details. The financial impact of such attacks is estimated to range from hundreds of millions to billions of dollars. Other intentional threats include electronic eavesdropping or scanning to uncover passwords and other data.

However, there are also unintentional threats that may be caused by flaws in computer software. From Chief Information Officers to students to small business owners, everyone must know how to respond to cyber attacks. When a new flaw is identified in ubiquitous software like Microsoft operating systems, users must take preemptive action to minimize damage from the inevitable hacker attacks. For example, security patches released by software manufacturers can be installed in systems to correct these flaws. When patches are announced, one has to act quickly to install them. So, does the average computer user know what software he is running? Does he know if the alert applies to him? If so, does he know where to find the patch and how to apply it? These are questions that the Committee is examining as part of the information security effort in the federal government.

The aggressive push to implement e-government initiatives means that federal computer systems are communicating with computers in homes and businesses (e.g., IRS e-filing). If non-federal computers are not adequately secured, there is added risk to our federal systems. The challenge for the federal government is to promote electronic government initiatives, while ensuring the integrity of its systems.

Educating public users about cyber security is critical. For many computer users, security is an issue they may address at work, but most people are lax about it when it comes to securing a home computer connected to the Internet. So the average user needs to understand how software such as peer-to-peer file sharing applications leave computers defenseless against cyber attacks. For instance, the recent Swen worm

circulating in Europe purports to be a Microsoft security alert and enters computers as an e-mail attachment or an e-mail delivery failure notice. Then it tries to spread to other computers through the Kazaa peer-to-peer file sharing network. Because of the interconnectivity of information systems and the increased reliance on computers for transactions via the Internet, this type of worm has the potential to cause significant damage to home computers as well as those in businesses, financial institutions, and governments.

Even our nation's critical infrastructure sectors depend on information systems to protect the nation's water supply, oil and gas pipelines, electrical grids, and other critical infrastructures. Significant damage to these systems could have a devastating impact on our national security, public health and safety, and economy. In fact, terrorists have already expressed their intent to attack our critical infrastructure, prompting the General Accounting Office to include cyber critical infrastructure protection on its high-risk series for the first time in January 2003.

Witnesses

Panel One:

- Ms. Karen Evans, Administrator, Office of Electronic Government, Office of Management and Budget

Panel Two:

- Dr. Tom Leighton, Co-Founder and Chief Scientist, Akamai Technologies, Inc.
- Mr. Kenneth Ammon, President and Co-Founder, NetSec

###